

**IN THE UNITED STATES DISTRICT COURT  
FOR THE WESTERN DISTRICT OF OKLAHOMA**

UNITED STATES OF AMERICA,	)	
	)	
Plaintiff,	)	
	)	
v.	)	Case No. CR-15-129-D
	)	
GREGORY JOHN MAUREK,	)	
	)	
Defendant.	)	

**ORDER**

Defendant Gregory Maurek has been indicted for receipt, distribution, and possession of child pornography. He moves to suppress all evidence acquired in the search of his computer [Doc. No. 15] on the grounds that (1) law enforcement’s use of the “Torrential Downpour” software program to access files from his computer constituted a warrantless search; and (2) the warrant authorizing the search lacked probable cause because the supporting affidavit neither disclosed the fact that “Torrential Downpour” was only accessible to law enforcement, nor did it describe the software’s technical or scientific reliability. The government filed its brief in opposition and an evidentiary hearing was held September 14, 2015. For the reasons stated below, Defendant’s motion is denied.

## BACKGROUND

As previously noted in this Court's Order of August 31, 2015 [Doc. No. 22], BitTorrent is a peer-to-peer ("P2P") file sharing network that is used to distribute large amounts of data over the Internet. BitTorrent is one of the most popular P2P networks used by individuals, as well as Ares, KaZaA, eDonkey, DirectConnect and Gnutella. *Warner Bros. Records, Inc. v. Does 1-4*, No. 2:07-cv-0424-TC, 2007 WL 1960602, at \*1, n. 10 (D. Utah July 5, 2007). As one court explained, since its release over ten 10 years ago:

BitTorrent has allowed users to share files anonymously with other users. Instead of relying on a central server to distribute data directly to individual users, the BitTorrent protocol allows individual users to distribute data among themselves by exchanging pieces of the file with each other to eventually obtain a whole copy of the file. When using the BitTorrent protocol, every user simultaneously receives information from and transfers information to one another. In the BitTorrent vernacular, individual downloaders/distributors of a particular file are called "peers." The group of peers involved in downloading/distributing a particular file is called a "swarm." A server which stores a list of peers in a swarm is called a "tracker." A computer program that implements the BitTorrent protocol is called a "BitTorrent client."

*First Time Videos, LLC v. Does 1-76*, 276 F.R.D. 254, 255 (N.D. Ill. 2011) (citations omitted). Also prominent in the BitTorrent lexicon are "torrents," small files which describe the file being shared/distributed. *Third Degree Films, Inc. v. Does 1-47*, No. 12-cv-2391-WJM-MEH, 2012 WL 4005842, at \*1 (D. Colo. Sep. 12, 2012). Torrents

contain information such as how the file is divided and other information needed for its distribution (e.g., name, description, etc.). *New Sensations, Inc. v. Does 1-426*, No. 12-3800-JSC, 2012 WL 4675281 at \*2 (N.D. Cal. Oct. 1, 2012). People may search for torrents for a specific work on the Internet; after a person finds a torrent, they may open the file with their BitTorrent client, and they then join the “swarm.” *Id.* In turn, as each peer receives portions of the file being downloaded, that peer usually makes those portions available to other peers in the swarm. *Id.* Consequently, each peer in the swarm is simultaneously copying and distributing pieces of the file. *Id.* One swarm may last for months up to well over a year, depending on the popularity of the work, and people may leave and re-enter the same swarm at any time. *Id.*

The challenged search warrant was based on an affidavit in which Kari Newman, a Special Agent with Homeland Security Investigations, asserted that an investigation of the activities of an IP address registered to Defendant’s residence established probable cause to believe someone at that address had received, possessed, and/or distributed child pornography over a P2P network. Agent Newman’s affidavit described how P2P file sharing works, how a user can search for specific files and connect directly with another user’s computer, and then download that file directly from the other user. She explained, in specific detail, the technological methods used by law enforcement to track down, identify, and arrest

suspected users/distributors of child pornography on P2P networks. Lastly, Agent Newman explained how digital media devices were being used to store child pornography and the requisite skill and knowledge necessary to search these devices for evidence.

The affidavit recounted the investigative steps that were taken to identify Defendant's computer. Agent Newman attested that on March 18, 2015, Detective Chris Lamer of the Moore Police Department conducted an online undercover investigation and he was able to connect with a computer with IP address 68.97.10.183 and download numerous files. Based on Agent Newman's review of the files, as well as her training and experience, she determined that the files depicted children under the age of eighteen engaged in sexually explicit conduct and thus constituted "child pornography" as that term is defined in 18 U.S.C. § 2256(8).

At the evidentiary hearing, the Court heard testimony from Robert Erdely, who teaches courses in online investigations of child pornography and participated in the development of Torrential Downpour. He testified that Torrential Downpour is a law enforcement surveillance software that is used exclusively by law enforcement. It is used to track, investigate, and eventually arrest those sharing child pornography through various P2P sharing networks. Mr. Erdely testified that Torrential Downpour is "somewhat unique" in that (1) it is designed to target and download files from a

single IP address, as opposed to multiple sources, and restrict downloads to come from only that particular address (this is called a “single source download”); (2) Torrential Downpour creates a detailed log of events for evidentiary purposes; and (3) Torrential Downpour does not share files. Mr. Erdely provided additional testimony on the overall nuances of Torrential Downpour and its role in the field of P2P file sharing. Of particular note, he stated Torrential Downpour’s direct connection capabilities were no different from other commercially available versions of BitTorrent and it (Torrential Downpour) had no rate of error.

Through a subpoena, Detective Lamer discovered the street address corresponding with the aforementioned IP address at the date and time of the downloads. He then conducted a search of the Oklahoma Department of Motor Vehicles records and confirmed that Defendant had a valid Oklahoma Driver’s License which listed him as residing at the same street address. The search warrant application was granted and upon execution of the warrant, agents seized and confiscated several digital storage devices from Defendant’s residence. Child pornography, consisting of both videos and still images, was found on a computer.

### **STANDARD**

The purpose of a suppression hearing is “to determine preliminarily the admissibility of certain evidence allegedly obtained in violation of defendant’s rights

under the Fourth and Fifth Amendments.” *United States v. Merritt*, 695 F.2d 1263, 1269 (10th Cir. 1982). “The proper inquiry is whether [the challenged action] violated the Fourth Amendment rights of [the] criminal defendant making the challenge.” *United States v. Allen*, 235 F.3d 482, 489 (10th Cir. 2000) (quoting *United States v. Erwin*, 875 F.2d 268, 270 (10th Cir.1989) (paraphrasing in original)). “The proponent of a motion to suppress has the burden of adducing facts at the suppression hearing indicating that his own rights were violated by the challenged search.” *United States v. Eckhart*, 569 F.3d 1263, 1274 (10th Cir. 2009) (quoting *Allen*, 235 F.3d at 489). The controlling burden of proof at a suppression hearing is proof by a preponderance of the evidence. *United States v. Matlock*, 415 U.S. 164, 177 n. 14, 94 S.Ct. 988, 996, 39 L.Ed.2d 424 (1974).

## DISCUSSION<sup>1</sup>

### I. WHETHER USE OF THE “TORRENTIAL DOWNPOUR” SOFTWARE CONSTITUTED A WARRANTLESS SEARCH

The Fourth Amendment protects only *reasonable* expectations of privacy. *Katz*

---

<sup>1</sup>The Court expresses no opinion on whether Defendant met the preliminary showing to require an evidentiary hearing under *Franks v. Delaware*, 438 U.S. 154, 172, 98 S.Ct. 2674, 57 L.Ed.2d 667 (1978). Rather, in its discretion, the Court determined an evidentiary hearing would be useful in resolving the present motion. See *United States v. Herrera*, 782 F.3d 571, 573-74 (10th Cir. 2015) (district court did not commit reversible error when it, *sua sponte*, allowed defendant a *Franks* hearing without requiring defendant to make threshold showing).

*v. United States*, 389 U.S. 347, 360, 88 S.Ct. 507, 516, 19 L.Ed.2d 576 (1967) (Harlan, J., concurring). Whether a defendant's Fourth Amendment rights were violated by a challenged search turns on the classic Fourth Amendment test: (1) whether the defendant manifested a subjective expectation of privacy in the area searched and (2) whether society is prepared to recognize that expectation as objectively reasonable. *United States v. Barrows*, 481 F.3d 1246, 1248 (10th Cir. 2007). "What a person knowingly exposes to the public, even in his own home or office, is not a subject of Fourth Amendment protection." *Katz*, 389 U.S. at 351 (citation omitted); *see also Smith v. Maryland*, 442 U.S. 735, 743-44, 99 S.Ct. 2577, 2582, 61 L.Ed.2d 220 (1979) ("a person has no legitimate expectation of privacy in information he voluntarily turns over to third parties.").

The Tenth Circuit, and numerous other federal courts, including this Court, have uniformly held there is no reasonable expectation of privacy in files made available to the public through peer-to-peer file-sharing networks. *See United States v. Brese*, No. CR-08-52-D, 2008 WL 1376269, at \*2 (W.D. Okla. Apr. 9, 2008) ("The Court finds that, notwithstanding any subjective expectation that Defendant may have had in the privacy of his computer, it was not reasonable for him to expect privacy in files that were accessible to anyone else with LimeWire (or compatible) software and an internet connection."); *United States v. Perrine*, 518 F.3d 1196, 1204-05 (10th Cir.

2008) (“Furthermore, as [defendant] conceded, he had peer-to-peer software on his computer, which permitted anyone else on the internet to access at least certain folders in his computer. To the extent such access could expose his subscriber information to outsiders, that additionally vitiates any expectation of privacy he might have in his computer and its contents.”); *United States v. Abston*, 401 Fed. App’x 357, 2010 WL 4367124 at \*\*6 (10th Cir. Nov. 5, 2010) (unpublished) (“An individual who has ‘enabled peer-to-peer file sharing on his computer, thereby giving anyone with internet access the ability to gain entrance to his computer ... holds no reasonable expectation of privacy that the Fourth Amendment will protect.’ ”) (quoting *Perrine*).<sup>2</sup>

As one court stated, “[r]ather than evidencing a subjective expectation of privacy, Defendant’s participation in the BitTorrent swarm demonstrates the exact opposite. By using peer-to-peer file sharing BitTorrent software, Defendant opened

---

<sup>2</sup>See also *United States v. Hill*, 750 F.3d 982, 986 (8th Cir. 2014); *United States v. Conner*, 521 Fed. App’x 493, 2013 WL 1490109 at \*\*3-4 (6th Cir. Apr. 11, 2013); (unpublished); *United States v. Norman*, 448 Fed. App’x 895, 897 (11th Cir. Oct. 4, 2011) (unpublished); *United States v. Borowy*, 595 F.3d 1045, 1047-48 (9th Cir. 2010); *United States v. Dodson*, 960 F. Supp. 2d 689, 695 (W.D. Tex. 2013); *United States v. Laduea*, No. 09-40021-FDS, 2010 WL 1427523, at \*4 (D. Mass. Apr. 7, 2010); *Columbia Pictures, Inc. v. Bunnell*, 245 F.R.D. 443, 452 (C.D. Cal. 2007) (“[e]ven if the users are engaged in *legal* file sharing, they have little to no expectation of privacy because they are broadcasting their identifying information to everyone in the BitTorrent ‘swarm’ as they download the file.”) (emphasis in original).



up his computer to allow other users of BitTorrent to access certain files to download. By opening his computer to the public, Defendant negates any claim he may have to subjective expectation of privacy in the files he made accessible to BitTorrent users online.” *United States v. Palmer*, No. 2:15-cr-1-FtM-38DNF, 2015 WL 4139069, at \*12 (M.D. Fla. July 8, 2015).

Defendant does not dispute that the files downloaded from his computer were found and shared over the BitTorrent P2P network. Defendant, therefore, has not established a reasonable, subjective expectation of privacy and his Motion to Suppress is overruled on this ground. Defendant’s attempt to distinguish the law enforcement version of the software as somehow different, or more invasive, than standard P2P programs does not alter the fact that he allowed public access to the files on his computer which contained images of child pornography, and thus compels no different conclusion.

## **II. WHETHER THE GOVERNMENT WAS REQUIRED TO DISCLOSE THE EXCLUSIVE NATURE OF TORRENTIAL DOWNPOUR AND PROVE ITS TECHNICAL AND SCIENTIFIC RELIABILITY**

Defendant’s failure to show a reasonable expectation of privacy effectively completes this Court’s analysis. *See Mahan v. Bunting*, No. 1:13-CV-00165, 2014 WL 1153444, at \*9 (N.D. Ohio Feb. 3, 2014)(“Where there is no reasonable expectation of privacy over the shared files, the technical aspects of the law

enforcement software are not at issue.”). Nonetheless, out of interests of completeness, the Court addresses his second proposition that the affidavit failed to establish probable cause due to deliberate or reckless omissions regarding the use of Torrential Downpour, namely, the fact it is only accessible to law enforcement and there was nothing that attested to the program’s technical or scientific reliability.

“A search warrant can issue only upon a showing of probable cause.” *United States v. Long*, 774 F.3d 653, 658 (10th Cir. 2014) (citing *United States v. Biglow*, 562 F.3d 1272, 1275 (10th Cir. 2009)). “The supporting affidavit must provide a substantial basis to conclude that there is a fair probability that contraband or evidence of a crime will be found in a particular place.” *Id.* (quoting *United States v. Nolan*, 199 F.3d 1180, 1182 (10th Cir.1999) (internal quotations omitted)). Courts examine the “totality of the circumstances” in the affidavit provided to determine whether it provided a substantial basis for finding a fair probability that contraband or other evidence of a crime would be found at the searched premises. *United States v. Myers*, 106 F.3d 936, 939 (10th Cir.1997). “[T]he Court must show deference to the magistrate’s finding of probable cause and must interpret the affidavit in a ‘common sense and realistic fashion.’ ” *United States v. Taylor*, No. 13–CR–0003–001–CVE, 2013 WL 2149644 at \*8 (N.D. Okla. May 16, 2013) (quoting *United States v. Grimmett*, 439 F.3d 1263, 1270 (10th Cir. 2006)).

A search warrant must be voided where a court: (1) finds that the affiant knowingly or recklessly included false statements in or omitted material information from an affidavit in support of a search warrant; and (2) concludes, after excising such false statements and considering such material omissions, that the corrected affidavit does not support a finding of probable cause. *United States v. Garcia-Zambrano*, 530 F.3d 1249, 1254 (10th Cir. 2008).

Information omitted from an affidavit is material only if it affects a finding of probable cause. *United States v. Kennedy*, 131 F.3d 1371, 1377 (10th Cir. 1997). In other words, “[w]hether the omitted statement was material is determined by examining the affidavit as if the omitted information had been included and inquiring if the affidavit would still have given rise to probable cause for the warrant.” *Stewart v. Donges*, 915 F.2d 572, 582 n. 13 (10th Cir. 1990); *see also United States v. Garza*, 980 F.2d 546, 551 (9th Cir. 1992) (refusing to suppress evidence when, “[e]ven if the misstatements were corrected and the omissions supplied, the affidavit would furnish probable cause for issuance of the warrant”).

In *United States v. Chiardio*, 684 F.3d 265 (1st Cir. 2012), the FBI undertook an undercover investigation to search for child pornography, which involved using the “LimeWire” software, which, like BitTorrent, is a commercially available P2P file sharing program that enables users to transmit files to and from other members of the

LimeWire network. Like BitTorrent, LimeWire users can search for files made available by other users, browse all the files made available by a particular user, and download desired files. *Chiardio*, 684 F.3d at 271. They can also make their own files accessible for download by designating a folder on their computers that would automatically share its contents with the network. *Id.*

The FBI developed and employed a special version of LimeWire, known as “enhanced peer-to-peer software” (EP2P), which was customized to assist child pornography investigations. The EP2P software differed from LimeWire in three principal respects:

First, when a user of the commercially available version of LimeWire tries to download a file, the program seeks out all the users who are sharing the same file and downloads different pieces of that file from multiple locations in order to optimize download speed. *EP2P eliminates that functionality; it allows downloading from **only one source at a time**, thus ensuring that the entire file is available on that source’s computer.* Second, in its commercially available iteration, LimeWire responds to a search term by displaying basic information such as the names of the available files, file types, and the file sharers’ Internet Protocol (IP) addresses. EP2P displays not only that data but also the identity of the Internet Service Provider (ISP) and the city and state associated with the IP address sharing a particular file. Third, EP2P has been modified so that an agent can easily compare the hash value (essentially, the digital fingerprint) of an available file with the hash values of confirmed videos and images of child pornography. *Taken together, these three modifications permit agents to download a file from **a single source**, learn the general location of the source, and facilitate the identification of child pornography as such.*

*Chiardio*, 684 F.3d at 271(emphasis added).<sup>3</sup> The FBI used the EP2P software to trace child pornography to a computer owned by the defendant, and he was subsequently indicted and convicted for possessing and distributing child pornography.

On appeal, the defendant contended, as here, that the search warrant affidavit lacked probable cause because it was based on “largely untested” software and the government did not sufficiently demonstrate the software’s reliability pursuant to *Daubert v. Merrell Dow Pharm., Inc.*, 509 U.S. 579, 597, 113 S.Ct. 2786, 125 L.Ed.2d 469 (1993).<sup>4</sup> The court overruled the motion by first noting that the Federal Rules of Evidence do not apply to proceedings surrounding the issuance of a search warrant, *Chiardio*, 684 F.3d at 279 (citing Fed. R. Evid. 1101(d)(3)), and that “probable cause ‘does not require scientific certainty.’ ” *Id.* (quoting *Roche v. John*

---

<sup>3</sup>EP2P’s ability to target a single source is obviously akin to Torrential Downpour’s ability to download from a single IP address.

<sup>4</sup>The *Daubert* factors, which are meant to assist trial courts in determining whether proposed expert testimony is based on reliable methods and principles, ask (1) whether the particular theory can be and has been tested; (2) whether the theory has been subjected to peer review and publication; (3) the known or potential rate of error; (4) the existence and maintenance of standards controlling the technique’s operation; and (5) whether the technique has achieved general acceptance in the relevant scientific or expert community. *Daubert*, 509 U.S. at 593-94. They are not a “definitive checklist or test,” but form the basis for a flexible inquiry into the overall reliability of a proffered expert’s methodology. *United States v. Baines*, 573 F.3d 979, 985 (10th Cir. 2009) (*Daubert*, 509 U.S. at 593).

*Hancock Mut. Life Ins. Co.*, 81 F.3d 249, 254 (1st Cir. 1996)). The court found the issuing magistrate had made a sensible determination, based on a detailed affidavit, that a search of the defendant's residence was likely to turn up illicit images. *Chiardio*, 684 F.3d at 279. This, the court determined, was sufficient to find probable cause.

The court also rejected the defendant's second contention, which also mirrors Defendant's challenge to *Torrential Downpour*, that the affidavit contained knowing or reckless material omissions about the reliability of EP2P. The First Circuit held the alleged omissions in the supporting affidavit were not material and had they been included, they would not have diluted the affidavit's showing of probable cause, but rather "had the affiant included the additional statements describing what was known about EP2P's reliability, those statements would have served no purpose except to strengthen the affidavit. It would be wildly illogical to suppress the fruits of a search on the ground that the warrant application omitted statements that, if included, would have *increased* the affidavit's persuasive force." *Id.* (citation omitted, emphasis in original).

The Court likewise overrules Defendant's contentions. The material fact law enforcement was obligated to disclose was its use of investigative technology to track, identify, and download the files from Defendant's computer. This fact was fully

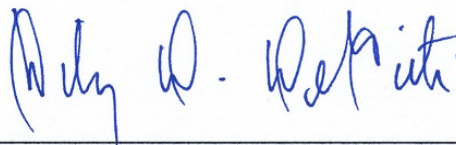
disclosed. More exacting details and disclosures simply were not required to establish probable cause. *See United States v. Biglow*, 562 F.3d 1272, 1280 (10th Cir. 2009) (“probable cause is a matter of ‘probabilities and common sense conclusions, not certainties.’”) (citations omitted). Defendant confuses the test for determining the admissibility of evidence from an expert witness at trial under Fed. R. Evid. 702 with the more flexible and less demanding standard for evidence necessary to establish probable cause. *See also Maryland v. Pringle*, 540 U.S. 366, 371, 124 S.Ct. 795, 800, 157 L.Ed.2d 769 (2003) (“The probable-cause standard is incapable of precise definition or quantification into percentages because it deals with probabilities and depends on the totality of the circumstances.”).

And, as the court observed in *Chiardio*, had more information about the intricacies of Torrential Downpour been included, these additional disclosures would not have affected the determination of probable cause because they would have merely provided the magistrate judge with further information regarding the source and capabilities of the automated software. Under the totality of the circumstances, the affidavit provided a substantial basis for the magistrate’s conclusion that there was probable cause for issuing the challenged warrant.

## **CONCLUSION**

Defendant's Motion to Suppress [Doc. No. 15] is **DENIED**.

**IT IS SO ORDERED** this 16<sup>th</sup> day of September, 2015.



---

TIMOTHY D. DEGIUSTI  
UNITED STATES DISTRICT JUDGE